

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

INFORMATION SHEET

Applicant(s): Thomas BIRKHOELZER; and Juergen VAUPEL

Application No: **NEW APPLICATION**

Filed: February 25, 2004

For: METHOD FOR SIGNING DATA

Priority Claimed Under 35 U.S.C. §119 and/or 120:

COUNTRY  
GERMANY

DATE  
February 25, 2003

NUMBER  
103 07 995.5

Send correspondence to : HARNESS, DICKEY & PIERCE, P.L.C.  
P.O. Box 8910  
Reston, VA 20195  
(703) 668-8000

The above information is submitted to advise the United States Patent and Trademark Office of all relevant facts in connection with the present application. A timely executed Declaration in accordance with 37 CFR 1.64 will follow.

Respectfully submitted,

By



Donald J. Daley  
Reg. No. 34,313  
P.O. Box 8910  
Reston, VA 20195  
(703) 668-8000

February 25, 2004  
DJD:jcp

**PATENT**  
32860-000703/US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: **NEW APPLICATION**  
Filing Date: February 25, 2004  
Applicants: Thomas BIRKHOELZER et al.  
Title: METHOD FOR SIGNING DATA

**PRIORITY LETTER**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

February 25, 2004

Dear Sirs:

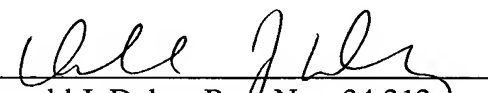
Pursuant to the provisions of 35 U.S.C. 119, enclosed is/are a certified copy of the following priority document(s).

<b><u>Application No.</u></b>	<b><u>Date Filed</u></b>	<b><u>Country</u></b>
103 07 995.5	2/25/2003	GERMANY

In support of Applicant's priority claim, please enter this document into the file.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By   
Donald J. Daley, Reg. No. 34,313

DJD:jcp

P.O. Box 8910  
Reston, Virginia 20195  
(703) 668-8000

Enclosure

# BUNDESREPUBLIK DEUTSCHLAND



## Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

**Aktenzeichen:** 103 07 995.5  
**Anmeldetag:** 25. Februar 2003  
**Anmelder/Inhaber:** Siemens Aktiengesellschaft,  
80333 München/DE  
**Bezeichnung:** Verfahren zum Signieren von Daten  
**IPC:** H 04 L 9/32

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 05. Februar 2004  
**Deutsches Patent- und Markenamt**  
**Der Präsident**  
Im Auftrag

Stark

## Beschreibung

## Verfahren zum Signieren von Daten

5 Die Erfindung betrifft ein Verfahren zum Signieren von Daten durch verschiedene Nutzer. Die Erfindung betrifft außerdem eine Datenverarbeitungseinrichtung zur Durchführung des Verfahrens sowie ein Speichermedium, auf dem Informationen zur Durchführung des Verfahrens auf einer Datenverarbeitungseinrichtung gespeichert sind.

Die zunehmende Nutzung elektronischer Daten und Kommunikationswege bringt ständig wachsende Anforderungen an Mechanismen zur nachträglichen Nachvollziehbarkeit von Datenzugriffen mit sich. Gleichzeitig soll jedoch eine möglichst einfache, bequeme und unaufwändige Zugreifbarkeit der Daten gewährleistet sein. Insbesondere aufgrund der zunehmenden gegenseitigen Vernetzung und der häufig großen Anzahl verschiedener Nutzer, die elektronischen Zugang zu den selben Daten erlangen können, sind wirksame elektronische oder software-basierte Dokumentations-Mechanismen unerlässlich geworden, um anonyme Manipulation oder Einsichtnahme zu verhindern.

Aufgrund der vielfältigen Zugriffsmöglichkeiten und aufgrund der Tatsache, dass elektronische Datenzugriffe nicht ohne weiteres auf real existierende Personen zurückgeführt werden können, ist es erforderlich, sämtliche Datenzugriffe unter Angabe einer Signatur des Zugreifenden zu speichern und damit zu dokumentieren. Die Dokumentation von Datenzugriffen durch real existierende Nutzer erfolgt durch Verwendung einer Nutzer-individuellen Signatur, die ausschließlich dem jeweiligen Nutzer zur Verfügung steht und zu deren Verwendung dieser sich authentifizieren muss.

35 Die Dokumentation von Zugriffen auf elektronische Daten spielt bei personenbezogenen Daten wie Adresslisten oder Kundendaten, bei Daten im Finanzwesen und insbesondere bei Daten

im Gesundheitswesen eine besonders wichtige Rolle. Im Gesundheitswesen, wo strengste Anforderungen an die Datensicherheit gestellt werden, fordern Datenschutzbestimmungen, dass jeder Nutzer von Daten eindeutig identifiziert und authentifiziert wird. Dabei bedeutet Identifizierung, dass jeder Datenzugriff bzw. jede Aktion eindeutig mit dem ausführenden Nutzer, also mit einer real existierenden Person, in Verbindung gebracht und mit einer elektronischen Signatur dieser Person zur nachträglichen Rekonstruierbarkeit dokumentiert wird. Authentifizierung bedeutet, dass die Authentifizierung eines Nutzer eigens geprüft wird und nur authentifizierten Nutzer überhaupt eine Signatur zugeteilt werden kann. Die Funktion der Dokumentation wird im Gesundheitswesen auch „auditing“ genannt, die Funktion der Authentifizierung auch „access control“.

Elektronische Daten können mehreren, verschiedenen Nutzern zur Verfügung stehen. Dies kann z.B. bei der Verwaltung von Kundendaten durch die Angestellten einer Bank der Fall sein, bei Personaldaten in Personalabteilungen, bei der gemeinsamen Nutzung von Daten in Entwicklungs-Teams oder bei Daten im Gesundheitswesen, die Teams von behandelnden Ärzten oder einem bestimmten Kreis medizinischen Fachpersonals zugänglich sein sollen. Sind mehrere Nutzer zur gemeinsamen Nutzung der selben Daten vorgesehen, so gehören sie diesbezüglich der selben Rolle an. Die gemeinsame Rollen-Zugehörigkeit spiegelt sich in den bekannten, nutzer-individuellen Signaturen nicht wieder. Insofern lässt sich die Rollen-Zugehörigkeit nicht mittels herkömmlicher Signaturen abbilden und muss, falls sie zur späteren Rekonstruierbarkeit dokumentiert werden soll, in geeigneter Weise eigens gespeichert und archiviert werden. Dies verkompliziert die für das „auditing“ erforderlichen Speichermaßnahmen erheblich. Auch die spätere Rekonstruktion von Datenzugriffen und deren Zuordnung zu Rollen-Zugehörigen ist dadurch umständlich.

Die Aufgabe der Erfindung besteht darin, die Verwendung von elektronischen Signaturen zu vereinfachen und gleichzeitig

eine vollständig nachträglich rekonstruierbare Dokumentation von Datenzugriffen verschiedener Nutzer und verschiedener Rollen-Zugehöriger auf gemeinsam genutzte elektronische Daten zu gewährleisten.

5

Die Erfindung löst diese Aufgabe durch ein Verfahren gemäß dem 1. Patentanspruch, durch eine Datenverarbeitungseinrichtung mit den Merkmalen des 9. Patentanspruchs und durch ein Speichermedium gemäß dem 16. Patentanspruch.

10

Ein Grundgedanke der Erfindung besteht darin, vor dem Signieren von Zugriffen auf elektronische Daten zunächst eine Sicherheitsabfrage zur Ermittlung der Identität eines Nutzers durchzuführen, und dem Nutzer in Abhängigkeit vom Ergebnis dieser Sicherheitsabfrage eine eindeutige Nutzer-Signatur und zusätzlich eine Rollen-Signatur zuzuteilen, wobei die Rollen-Signatur mehreren, verschiedenen Nutzern zugeteilt werden kann. Das Signieren von Daten-Zugriffen erfolgt unter Angabe der Nutzer-Signatur und zusätzlich der Rollen-Signatur. Weder die Nutzer-Signatur noch die Rollen-Signatur sind für den Nutzer einsehbar.

20

Durch die Signierung von Datenzugriffen unter Angabe sowohl der Nutzer- als auch der Rollen-Signaturen ergibt sich der Vorteil, dass alle Informationen zur späteren Rekonstruktion der Identität und der Rolle eines Datenzugreifenden zum Zeitpunkt des Datenzugriffs durch die Signatur gegeben sind. Darüber hinaus sind die Signaturen weitestgehend sicher vor Manipulationen, da sie in Abhängigkeit von einer Sicherheitsabfrage zugeteilt werden und für den Nutzer nicht einsehbar und deshalb nicht durch ihn missbrauchbar sind. Ein weiterer Vorteil besteht darin, dass das Verfahren vom Nutzer lediglich eine Sicherheitsabfrage erfordert, im übrigen aber für den Nutzer grundsätzlich unbemerkt abläuft, und daher besonders einfach und unaufwändig handhabbar ist.

30

35

In einer vorteilhaften Ausgestaltung der Erfindung erfolgt die Sicherheitsabfrage durch biometrische Ermittlung von Nutzer-Daten, wie z.B. die Erfassung der Gestalt der Iris oder des Fingerabdrucks. Dadurch ergibt sich der Vorteil, dass eine besonders hohe Täuschungssicherheit erzielt wird, ohne vom Nutzer zusätzlichen Aufwand wie z.B. das Memorieren eines Passwortes zu erfordern.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung erfolgt die Ermittlung der Nutzer-Signatur durch Abfrage eines Nutzer-Signatur-Speichers, der räumlich entfernt angeordnet ist. Dadurch ergibt sich der Vorteil, dass der Nutzer-Signatur-Speicher durch eine eigens dafür vorgesehene Administration gepflegt und mittels besonders restriktiver Schutzmaßnahmen, z.B. Firewalls, geschützt werden kann, denen der Arbeitsplatz des Nutzers nicht zu unterliegen braucht. Ebenso kann der Rollen-Signatur-Speicher räumlich entfernt angeordnet werden, um die gleichen Vorteile zu erzielen, wobei er zusammen mit oder getrennt von dem Nutzer-Signatur-Speicher angeordnet sein kann.

Eine weitere vorteilhafte Ausgestaltung der Erfindung ergibt sich dadurch, dass jedem Nutzer zwar nur eine Nutzer-Signatur, jedoch mehrere Rollen-Signaturen gleichzeitig zugeordnet werden können. Dies spiegelt die tatsächlichen Rollen-Zugehörigkeiten wieder, da ein Nutzer z.B. in mehreren Funktionen oder als Mitglied mehrerer Teams, die jeweils eigene Rollen darstellen, tätig sein kann. Aus der Möglichkeit, mehreren Rollen-Signaturen anzugehören, ergibt sich der Vorteil, dass die realen Rollen-Zugehörigkeiten vollständig durch die Signaturen abgebildet werden können.

Vorteilhafte Ausgestaltungen der Erfindung sind Gegenstand der abhängigen Patentansprüche.

Nachfolgend werden Ausführungsbeispiele der Erfindung anhand von Figuren näher erläutert. Es zeigen:

FIG 1        Flussdiagramm mit den zur Ausführung der Erfindung erforderlichen Verfahrensschritten,

5    FIG 2        zur Ausführung der Erfindung geeignete Systemarchitektur.

10    **Figur 1** zeigt die Verfahrensschritte, die zur Ausführung der Erfindung erforderlich sind.

15    In Schritt 1 wird die Datenverarbeitungseinrichtung 50, die z.B. ein medizinischer Computer-Arbeitsplatz sein kann, gestartet. Dabei erfolgt das übliche Starten eines Betriebssystems und die Anmeldung daran. Das Verfahren zum Signieren gemäß der Erfindung verläuft jedoch unabhängig von einer solchen Anmeldung am Betriebssystem.

20    In Schritt 3 wird das Signatur-Tool 51 im Anschluss an das Hochfahren des Betriebssystems gestartet. Das Signatur-Tool 51 muss nicht mit jedem Hochfahren des Betriebssystems gestartet werden, es ist jedoch sichergestellt, dass es vor jeglichem Datenzugriff auf Applikationsdaten des Arbeitsplatzes gestartet wird. Bei den Applikationsdaten kann es sich  
25    z.B. um diagnostische Aufnahmen, medizinische Befunde, Persönlichkeitsinformationen von Patienten, aber auch um forschungsrelevante Inhalte, demographische Informationen oder um Finanzinformationen handeln. Bei all diesen Beispielen handelt es sich um kritische Daten, deren Zugriffe in besonderer Weise zu dokumentieren sind.  
30

35    In Schritt 5 erfolgt eine Sicherheitsabfrage, mittels derer ein Nutzer identifiziert werden soll. Dazu werden vom Nutzer personen-individuelle Daten erfragt, die allen Anforderungen an die Datensicherheit genügen müssen. Vorzugsweise wird dazu ein Sicherheitsabfrage-Mittel 59 angesprochen, durch das eine biometrische Erfassung von charakteristischen und möglichst



täuschungssicheren Daten wie Fingerabdruck oder Gestalt der Iris erfolgt. Daneben besteht die Möglichkeit, dass das Sicherheitsabfrage-Mittel 59 eine elektronische Chipkarte oder einen elektronischen oder mechanischen Schlüssel ausliest.

- 5 Durch die Sicherheitsabfrage wird den Anforderungen an die Authentifizierung Rechnung getragen.

10 In Schritt 6 besteht die Möglichkeit, das Verfahren nach Fehlschlagen der Sicherheitsabfrage abubrechen, um einem erhöhten Bedürfnis nach Datensicherheit gerecht zu werden.

15 In Schritt 7 wird ein Nutzer-Signatur-Speicher 61 abgefragt. Im Nutzer-Signatur-Speicher 61 sind Informationen abgelegt, mittels derer ein Nutzer anhand der in der vorangegangenen Sicherheitsabfrage ermittelten Daten als real existierende Person identifiziert werden kann. Die Nutzer-Signatur könnte zum Beispiel einer tabellarischen Zuordnung zwischen Signaturen und Sicherheitsabfrage-Daten zu entnehmen sein, oder einer Zuordnung zu im Ergebnis der Sicherheitsabfrage identifizierten real existierenden Personen.

25 In Schritt 9 wird im Ergebnis der vorangegangenen Abfrage des Nutzer-Signatur-Speichers 61 eine Nutzer-Signatur ermittelt. Der Grad der Täuschungssicherheit bei der Ermittlung der Nutzer-Signatur hängt im wesentlichen von der Täuschungssicherheit der vorangegangenen Sicherheitsabfrage sowie der Manipulierbarkeit des Nutzer-Signatur-Speichers 61 ab.

30 In Schritt 11 wird die vorangehend ermittelte Nutzer-Signatur dem aktuellen Nutzer zugeteilt und steht ab sofort zur Signierung von Aktionen des Nutzers zur Verfügung. Die Zuteilung erfolgt für den Nutzer grundsätzlich unbemerkt, insbesondere wird keinerlei Möglichkeit zur Einsichtnahme in die Signatur gegeben. Dadurch wird der Nutzer zu einem nicht mit für ihn unwichtigen Informationen belastet, zum anderen wird durch die Unkenntnis verhindert, dass er die Signatur missbräuchlich einsetzen kann.

In Schritt 13 wird ein Rollen-Signatur-Speicher 63 abgefragt. Im Rollen-Signatur-Speicher 63 sind Informationen abgelegt, mittels derer eine sogenannte Rolle anhand der in der vorangegangenen Sicherheitsabfrage ermittelten Daten identifiziert werden kann. Dazu könnte zum Beispiel auf eine tabellarische Zuordnung zwischen Rollen und Sicherheitsabfrage-Daten zugegriffen werden. Statt einer Zuordnung zu Sicherheitsabfrage-Daten könnte auch eine Zuordnung zu Nutzer-Signaturen oder zu im Ergebnis der Sicherheitsabfrage identifizierten real existierenden Personen verwendet werden.

Mit Rolle ist Zugehörigkeit zu einem bestimmten Tätigkeitskreis mit einer bestimmten Verantwortlichkeit gemeint, z.B. „Diensthabender Arzt“, „Medizinisch-technischer Assistent“, „Behandelndes Team“, „System-Administrator“, „Personalabteilung“ oder „Projektleiter“.

Die Rollen-Zugehörigkeit kann sich entweder objektbezogen ergeben, d.h. aus dem Bedürfnis bestimmter Nutzer, mit einem bestimmten Datenbestand arbeiten zu können, oder subjektbezogen, d.h. aus einer hierarchischen Einstufung des jeweiligen Nutzer, aufgrund derer er auf Daten einer bestimmten Einstufung zugreifen darf. Außerdem kann ein Nutzer mehreren Rollen angehören, die z.B. verschiedene „Behandelnde Teams“ repräsentieren, in denen der Nutzer gleichzeitig mitarbeitet. In solchen Fällen könnte der Nutzer entweder eine einzige Rollen-Signatur zugeteilt bekommen, die alle Rollen-Zugehörigkeiten repräsentiert, oder er könnte mehrere Rollen-Signaturen gleichzeitig zugeteilt bekommen.

In Schritt 15 wird im Ergebnis der vorangegangenen Abfrage des Rollen-Signatur-Speichers 63 eine Rolle oder gegebenenfalls eine Mehrzahl von Rollen ermittelt.

In Schritt 17 wird im Ergebnis der Ermittlung einer oder mehrerer Rollen eine oder gegebenenfalls eine Mehrzahl von zugehörigen Rollen-Signaturen ermittelt.

5 Die Aufteilung der vorangegangenen Schritt 15 und 17 spiegelt ein Vorgehen bei der Ermittlung von Rollen und Rollen-Signaturen wieder, bei dem zunächst aufgrund der Erfordernisse das Arbeitsumfeldes Rollen und Rollen-Zugehörigkeiten definiert und anschließend für diese Rollen elektronische Signaturen definiert werden. Die Schritte 15 und 17 könnten jedoch auch in einen einzigen Schritt integriert werden, indem auf den Zwischenschritt der Ermittlung einer oder mehrerer Rollen verzichtet wird und stattdessen Rollen-Signaturen sofort ermittelt werden.

15

In Schritt 19 wird die vorangehend ermittelte Rollen-Signatur oder die Mehrzahl von Rollen-Signaturen dem aktuellen Nutzer zugeteilt und steht ab sofort zur Signierung von Aktionen des Nutzers zur Verfügung. Die Zuteilung erfolgt, wie oben erläutert, für den Nutzer grundsätzlich unbemerkt, insbesondere erhält er keinerlei Möglichkeit zur Einsichtnahme in die Signatur.

20

25 In Schritt 21 werden Aktionen sowohl mit der zugeteilten Nutzer-Signatur als auch mit der oder den zugeteilten Rollen-Signaturen signiert. Die mehrfache Signierung erlaubt die vollständige nachträgliche Rekonstruktion aller signierten Datenzugriffe in Zuordnung sowohl zu einer real existierenden Person als auch in Zuordnung zu deren jeweils aktueller Rollen-Zugehörigkeit. Dadurch wird den Anforderungen an das Auditing von Datenzugriffen genüge getan, ohne dass zum Beispiel zusätzliche Informationen wie in der Vergangenheit liegende Dienstpläne abgefragt werden müssten, um die ehemaligen Rollen-Zugehörigkeiten von Personen nachträglich zu rekonstruieren.

30

35

In **Figur 2** ist eine elektronische Datenverarbeitungseinrichtung 50 dargestellt, die das Verfahren zur Ausführung der Erfindung ausführen kann. Die Datenverarbeitungseinrichtung 50 weist eine Tastatur 55 oder ein sonstiges Eingabegerät sowie  
5 einen Bildschirm 53 auf. Je nach Art der Anwendung können auch akustische Ein- und Ausgangssignale verarbeitet werden. Art und Umfang der Ein- und Ausgabegeräte sind für die Ausführung der Erfindung nicht von Belang. Bei der Datenverarbeitungseinrichtung 50 kann es sich sowohl um einen medizinischen Arbeitsplatz, z.B. eine sogenannte Modalität, als auch  
10 um einen beliebigen anderen Bildschirmarbeitsplatz, z.B. ein Bankterminal, handeln.

Die Datenverarbeitungseinrichtung 50 weist ein Signatur-Tool  
15 51 auf. Das Signatur-Tool 51 kann modular in die Datenverarbeitungseinrichtung 50 integrierbar sein, z.B. als einsteckbare Karte oder als Computer-Programm. Über das Signatur-Tool 51 hat die Datenverarbeitungseinrichtung 50 Zugriff auf einen Applikationsdaten-Speicher 57, der der Speicherung von Anwendungs-Daten dient.  
20

Das Signatur-Tool 51 und die Datenverarbeitungseinrichtung 50 sind derart konzipiert, dass ein Zugriff auf den Applikationsdaten-Speicher 57 ausschließlich über das Signatur-Tool 51  
25 erfolgen kann. Dadurch ist sichergestellt, dass jeglicher Datenzugriff ohne Umgehungsmöglichkeit durch das Signatur-Tool 51 dokumentiert und signiert wird. Dadurch sind Manipulation oder Missbrauch durch Umgehen des Signiervorgangs weitestgehend unmöglich.

Das Signatur-Tool 51 ist mit einem Sicherheitsabfrage-Mittel  
30 59 verbunden, das der Ermittlung von Daten zur Identifikation des jeweiligen Nutzers dient. Das Sicherheitsabfrage-Mittel 59 kann ein Chipkartenleser sein, der eine Nutzer-  
35 individuelle Chipkarte ausliest. Es kann auch ein mechanisches oder elektronisches Schloss sein, das einen Nutzer-individuellen Schlüssel ausliest. Nicht zuletzt kann es ein

Sensor zur Ermittlung biometrischer Daten des Nutzers sein, die beispielsweise die Gestalt von dessen Iris, dessen Fingerabdrücke oder dessen Sprach-Frequenzspektrum misst. Die Verwendung biometrischer Daten im Rahmen der Sicherheitsabfrage weist den Vorteil auf, dass keinerlei Schlüssel oder Karte verwendet werden muss, die der Nutzer verlieren oder die ihm entwendet werden könnten. Darüber hinaus ist die Täuschungssicherheit biometrischer Daten höher einzuschätzen als die von sonstigen Schlüsselsystemen.

10

Das Signatur-Tool 51 hat weiter Zugriff auf einen Nutzer-Signatur-Speicher 61, der Informationen zur Identifikation von Nutzern anhand der durch das Sicherheitsabfrage-Mittel 59 ermittelten Daten enthält. Diese Informationen ermöglichen es, eine Nutzer-Signatur zu ermitteln, z.B. aufgrund tabellarischer Zuordnungen zwischen Sicherheitsabfrage-Daten und Signaturen. Außerdem kann der jeweilige Nutzer anhand dieser Informationen als real existierende Person identifiziert werden.

20

Das Signatur-Tool 51 hat außerdem Zugriff auf einen Rollen-Signatur-Speicher 63, der Informationen zur Ermittlung einer oder mehrerer Rollen-Signaturen anhand der durch das Sicherheitsabfrage-Mittel 59 ermittelten Daten enthält. Diese Informationen ermöglichen es, eine Rollen-Signatur zu ermitteln, z.B. aufgrund tabellarischer Zuordnungen von Rollen-Signaturen zu Sicherheitsabfrage-Daten, zu real existierenden Personen oder zu Nutzer-Signaturen.

Für die Signatur-Speicher 61, 63 gelten besondere Sicherheitsanforderungen, die eine entfernt angeordnete, zentrale Aufstellung dieser Speicher sinnvoll machen können. Zu diesem Zweck sind sie unabhängig von der Datenverarbeitungseinrichtung 50 und dem Signatur-Tool 51 positionierbar und könnten beispielsweise auch über geschützte Datenfernverbindungen zugreifbar sein. Mit Datenfernverbindung kann eine kabellose

oder kabelgebundene Modem-Verbindung ebenso wie z.B. eine Internet- oder Intranet-Verbindung gemeint sein.

Die unabhängige Positionierung der Signatur-Speicher 61, 63 ermöglicht zum einen deren Zugreifbarkeit auch für weitere, andere Datenverarbeitungseinrichtungen oder Signatur-Tools. Zum anderen ermöglicht sie die Einrichtung strengerer Sicherheitsvorkehrungen speziell für die Signatur-Speicher 61, 63 im Vergleich zur Datenverarbeitungseinrichtung 50, z.B. eines besonders restriktiven Fire-Walls.

Die Verwendung von zwei getrennten Signatur-Speichern 61, 63 verleiht dem Signierungs-System einen modularen Aufbau mit größtmöglicher Flexibilität. Dadurch können in den Signatur-Speichern 61, 63 jederzeit weitgehend unabhängig voneinander Änderungen vorgenommen werden. Im Nutzer-Signatur-Speicher 61 können die zur Identifikation des Nutzers verwendeten, sicherheitskritischen Informationen regelmäßig geändert werden, in Anlehnung an die getrennte Aufstellung zentraler Trust-Center. Im Rollen-Signatur-Speicher 63 können Änderungen der Rollen-Zugehörigkeit vorgenommen werden, die die Veränderungen in der Zugehörigkeit realer Personen zu Teams oder Verantwortlichkeiten widerspiegeln.

Vorangehend wurde das Signierungs-System auf Basis der Verwendung von zwei unterschiedlichen Signatur-Speichern 61, 63 beschrieben. Diese zwei Speicher repräsentieren die logischen Zuordnungen von Informationen, die im Ablauf des Signierungs-Verfahrens getroffen werden. Zum ersten muss der Nutzer bzw. dessen Nutzer-Signatur im Ergebnis der Sicherheitsabfrage identifiziert werden, zum zweiten muss er einer Rolle zugeordnet bzw. eine Rollen-Signatur ermittelt werden.

Obwohl der modulare Aufbau die tatsächlichen logischen Zuordnungen korrekt repräsentiert, wäre es jedoch selbstverständlich möglich, stattdessen einen einzigen, integrierten Signatur-Speicher zu verwenden. Dieser einzige Signatur-Speicher

könnte je nach den sonstigen Anforderungen getrennt angeordnet oder in das Signatur-Tool 51 oder die Datenverarbeitungseinrichtung 50 integriert sein.

- 5 Wesentlich ist jedoch, dass die Sicherheitsabfrage durch das Sicherheitsabfrage-Mittel 59 keinen Rückschluss auf die zuzuteilenden Signaturen gestattet, die zur Signierung von Nutzer-Aktionen verwendet werden. Dies ist Garant dafür, dass die verwendete Signatur nicht manipulierbar und zuverlässig  
10 ist.

- Das Signatur-Tool 51 dokumentiert jeglichen Zugriff auf Applikationsdaten bzw. den Applikationsdaten-Speicher 57 unter Angabe der Nutzer-Signatur und zusätzlich der Rollen-  
15 Signatur. Sind mehrere Rollen-Signaturen zugeteilt, so werden auch diese zu Dokumentationszwecken angegeben. Sämtliche Signaturen werden durch das Signatur-Tool 51 zusammen mit Informationen über die zugegriffenen Daten und über die Art des Datenzugriffs gespeichert. Dadurch kann jederzeit im Nachhi-  
20 nein rekonstruiert werden, wer in welcher Weise auf welche Daten zugegriffen hat. Darüber hinaus kann die jeweils aktuelle Rolle des Datenzugreifenden anhand der Rollen-Signatur bzw. -Signaturen festgestellt werden, ohne dass dazu weitere Informationen, z.B. archivierte Dienstpläne oder Anwesen-  
25 heitslisten, eingeholt werden müssten. Durch die Sicherheitsabfrage 5 ist dabei jederzeit sichergestellt, dass die zur Dokumentation verwendeten Signaturen korrekt zugeteilt werden.

- 30 Darüber hinaus erhält der Nutzer keinerlei Einsicht in die durch das Signatur-Tool 51 verwendeten Signaturen. Dadurch werden die Möglichkeiten zu Missbrauch und Manipulation der Signatur-Daten weitestgehend vermieden. Darüber hinaus wird der Nutzer mit dem Zuteilen der Signaturen nicht weiter kon-  
35 frontiert und erfährt das Arbeiten des Signatur-Tools 51 als unaufwändig und einfach handhabbar.

Die Dokumentation der Datenzugriffe durch das Signatur-Tool 51 erfolgt grundsätzlich zusammen mit den zugegriffenen Applikationsdaten im Applikationsdaten-Speicher 57. Zusätzlich kann ein Audit-Speicher 65 zur getrennten Dokumentation aller

5 Nutzer-Aktionen vorgesehen sein. Dadurch wird die Möglichkeit geschaffen, im Audit-Speicher 65 z.B. lediglich die Art der Datenzugriffe sowie die Signaturen zu speichern, auf die Speicherung der möglicherweise sehr umfänglichen Applikationsdaten jedoch zu verzichten. Insbesondere medizinische

10 Bilddaten weisen häufig einen beträchtlichen Speicherumfang auf, der eine Auslagerung in Archivsysteme erforderlich machen kann. Der getrennte Audit-Speicher 65 kann in solchen Fällen dazu dienen, eine arbeitsplatz-spezifische Anwendungshistorie aufzuzeichnen, um neben Zugriffen auf die Applikationsdaten auch die Benutzung des jeweiligen Arbeitsplatzes

15 nachträglich rekonstruierbar zu dokumentieren, ohne jedoch die gesamten speicherintensiven Anwendungsdaten speichern zu müssen.



## Patentansprüche

1. Verfahren zum Signieren von Zugriffen auf elektronische Daten, wobei in einem ersten Schritt (5) eine Sicherheitsabfrage zur Ermittlung der Identität eines Nutzers durchgeführt wird, wobei in einem zweiten Schritt (11) in Abhängigkeit vom Ergebnis der Sicherheitsabfrage eine den Nutzer eindeutig identifizierende Nutzer-Signatur für den Nutzer nicht einsehbar zuteilbar ist, wobei in einem dritten Schritt (19) in Abhängigkeit vom Ergebnis der Sicherheitsabfrage eine Rollen-Signatur für den Nutzer nicht einsehbar zuteilbar ist, die mehreren Nutzern zuteilbar ist, und wobei in einem vierten Schritt (21) ein Zugriff auf elektronische Daten unter Angabe der Nutzer-Signatur und der Rollen-Signatur signierbar ist.

15

2. Verfahren nach Anspruch 1,  
dadurch gekennzeichnet, dass in der Sicherheitsabfrage biometrische Daten des Nutzers ermittelt werden.

20

3. Verfahren nach einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet, dass in der Sicherheitsabfrage ein elektronischer und/oder mechanischer Schlüssel ausgelesen wird.

25

4. Verfahren nach einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet, dass die zuzuteilende Nutzer-Signatur anhand der in der Sicherheitsabfrage ermittelten Daten durch Abfrage eines Nutzer-Signatur-Speichers (61) ermittelbar ist.

30

5. Verfahren nach einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet, dass die zuzuteilende Rollen-Signatur anhand der in der Sicherheitsabfrage ermittelten Daten durch Abfrage eines Rollen-Signatur-Speichers (63) ermittelbar ist.

35

6. Verfahren nach Ansprüche 4 oder 5,  
dadurch gekennzeichnet, dass die Abfra-  
ge des Nutzer-Signatur-Speichers (61) und/oder des Rollen-  
Signatur-Speichers (63) über eine Datenfernverbindung er-  
5 folgt.

7. Verfahren nach einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet, dass einem Nut-  
zer mehrere Rollen-Signaturen gleichzeitig zuteilbar sind.

10

8. Verfahren nach einem der vorhergehenden Ansprüche,  
dadurch gekennzeichnet, dass die Daten  
medizinisch relevant sind, dass die Nutzer medizinisches  
Fachpersonal sind, und dass die Rollen entsprechend den Ar-  
15 beits-Gruppen innerhalb des medizinischen Fachpersonals ge-  
bildet werden.

20

9. Datenverarbeitungseinrichtung (50) mit einem Signatur-Tool  
(51) und einem Sicherheitsabfrage-Mittel (59), wobei vor ei-  
nem Zugriff der Datenverarbeitungseinrichtung (50) auf Appli-  
kationsdaten durch das Sicherheitsabfrage-Mittel (59) eine  
Sicherheitsabfrage zur Ermittlung der Identität eines Nutzers  
durchführbar ist, wobei durch das Signatur-Tool (51) in Ab-  
hängigkeit von einem Ausgangssignal des Sicherheitsabfrage-  
25 Mittels (59) eine den Nutzer eindeutig identifizierende Nut-  
zer-Signatur für den Nutzer nicht einsehbar zuteilbar ist,  
wobei durch das Signatur-Tool (51) in Abhängigkeit von einem  
Ausgangssignal des Sicherheitsabfrage-Mittels (59) eine Rol-  
len-Signatur für den Nutzer nicht einsehbar zuteilbar ist,  
30 die mehreren Nutzen zuteilbar ist, und wobei durch das Signa-  
tur-Tool (51) Zugriffe auf elektronische Daten unter Angabe  
der Nutzer-Signatur und der Rollen-Signatur signierbar sind.

35

10. Datenverarbeitungseinrichtung (50) nach Anspruch 9,  
dadurch gekennzeichnet, dass durch das  
Sicherheitsabfrage-Mittel (59) biometrische Daten des Nutzers  
ermittelbar sind.

11. Datenverarbeitungseinrichtung (50) nach Anspruch 9 oder 10,

5 d a d u r c h g e k e n n z e i c h n e t , dass durch das Sicherheitsabfrage-Mittel (59) elektronische und/oder mechanische Schlüssel auslesbar sind.

12. Datenverarbeitungseinrichtung (50) nach Anspruch 9, 10 oder 11,

10 d a d u r c h g e k e n n z e i c h n e t , dass das Signatur-Tool (51) Zugriff auf einen Nutzer-Signatur-Speicher (61) hat, aus dem in Abhängigkeit von einem Ausgangssignal des Sicherheitsabfrage-Mittels (59) die zuzuteilende Nutzer-Signatur abfragbar ist.

15

13. Datenverarbeitungseinrichtung (50) nach Anspruch 9, 10, 11 oder 12,

20 d a d u r c h g e k e n n z e i c h n e t , dass das Signatur-Tool (51) Zugriff auf einen Rollen-Signatur-Speicher (63) hat, aus dem in Abhängigkeit von einem Ausgangssignal des Sicherheitsabfrage-Mittels (59) die zuzuteilende Rollen-Signatur abfragbar ist.

14. Datenverarbeitungseinrichtung (50) nach Anspruch 12 oder 13,

25 d a d u r c h g e k e n n z e i c h n e t , dass der Nutzer-Signatur-Speicher (61) und/oder der Rollen-Signatur-Speicher (63) von der Datenverarbeitungseinrichtung (50) entfernt angeordnet ist und dass das Signatur-Tool (51) über eine Datenfernverbindung darauf Zugriff hat.

30

15. Datenverarbeitungseinrichtung (50) nach Anspruch 9, 10, 11, 12, 13 oder 14,

35 d a d u r c h g e k e n n z e i c h n e t , dass sie ein medizinischer Arbeitsplatz ist.

16. Speichermedium, auf dem Information gespeichert ist, die in Wechselwirkung mit einer Datenverarbeitungseinrichtung (50) treten kann, um das Verfahren nach einem der Ansprüche 1 bis 8 auszuführen.

## Zusammenfassung

## Verfahren zum Signieren von Daten

- 5 Die Erfindung betrifft ein Verfahren zum Signieren von Zugriffen auf elektronische Daten sowie eine Datenverarbeitungseinrichtung zur Ausführung des Verfahrens. In einem ersten Schritt (5) des Verfahrens wird eine Sicherheitsabfrage zur Ermittlung der Identität eines Nutzers durchgeführt. In
- 10 einem zweiten Schritt (11) wird in Abhängigkeit vom Ergebnis der Sicherheitsabfrage eine den Nutzer eindeutig identifizierende Nutzer-Signatur für den Nutzer nicht einsehbar zugeteilt. In einem dritten Schritt (19) wird in Abhängigkeit vom Ergebnis der Sicherheitsabfrage eine Rollen-Signatur für den
- 15 Nutzer nicht einsehbar zugeteilt, die mehreren Nutzern mit gemeinsamer Rollenzugehörigkeit parallel zuteilbar ist. In einem vierten Schritt (21) werden Zugriffe auf elektronische Daten unter Angabe sowohl der Nutzer-Signatur als auch der Rollen-Signatur signiert. Durch die mehrfache Signatur ist
- 20 die nachträgliche Rekonstruktion sämtlicher Datenzugriffe unter Angabe der Nutzers und der Rollenzugehörigkeit des Nutzers zum Zeitpunkt des Datenzugriffs gewährleistet.

FIG 1

FIG 1

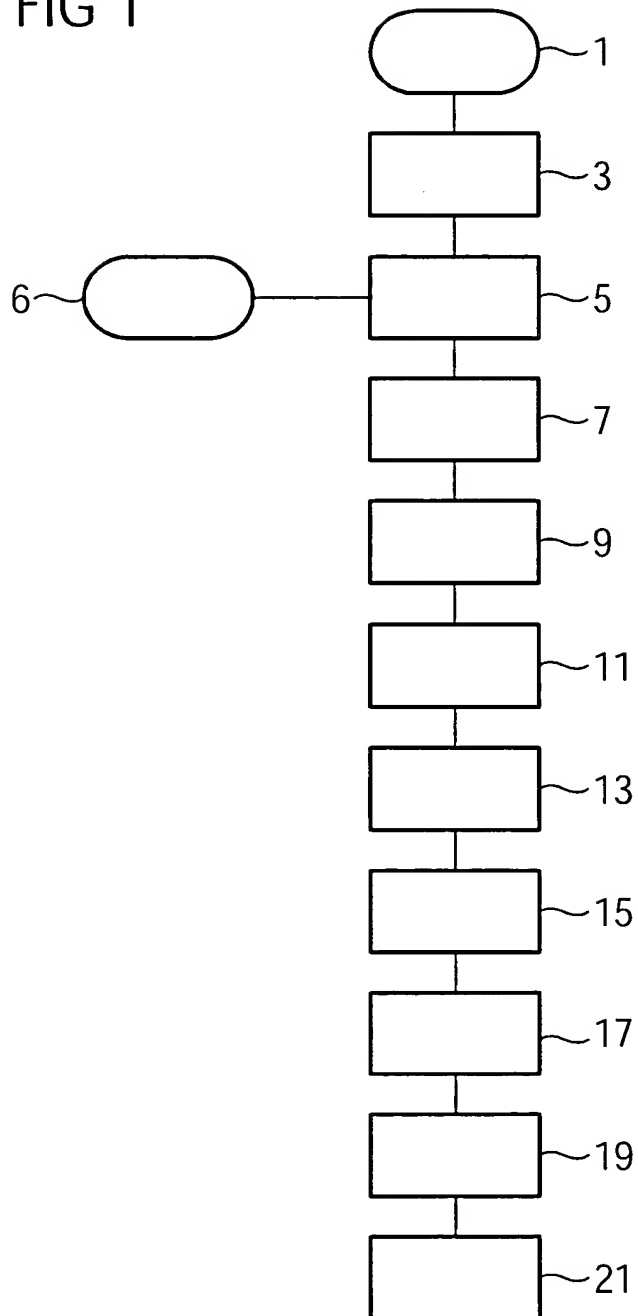


FIG 2

